RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART4-T10

Under Siege: How APTs and Nation-States Are Coming for Everyone

Eric Chien & Jason Rolleston

Enterprise Security Group at Broadcom

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

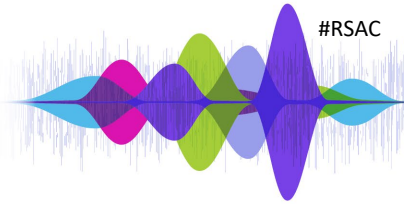
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC | 2025 Conference

01
Under Siege

Not So Long Ago



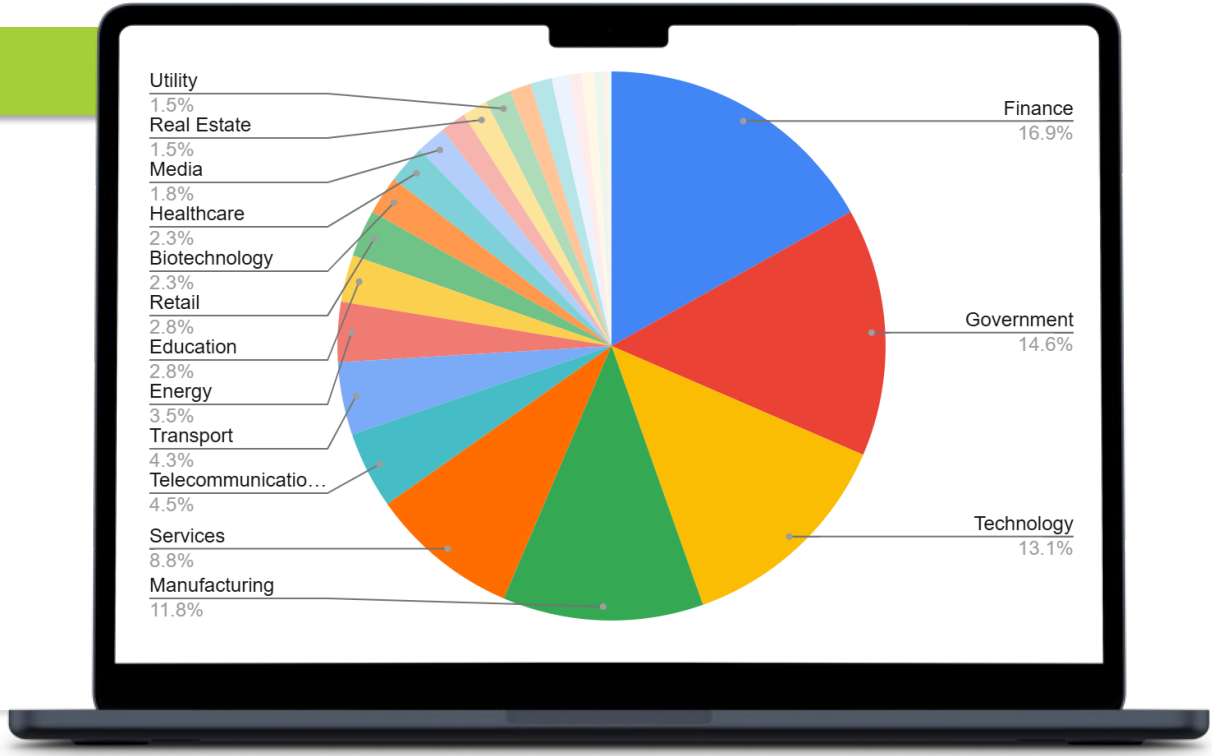
Only Government Entities or the Largest Enterprises needed to Worry About Advanced Threat Actors

Emerging Trend

State actors widen targeting

SMBs now in the firing line

- Historically focus on:
  - Governments
  - Military
  - Large Corporations
- Now, organizations off all sizes are targeted. Why?
  - Proliferation of attacks
  - Deep supply chain, wider net
  - Financially motivated attacks



China

Vast cyber operations

Multiple groups, highly active

Significant overlap of tooling/ infrastructure suggesting shared resources and use of contractors

Capable of targeting governments right down to SMBs

Recently…

Economic espionage or foothold attacks against SMB organizations

Moonlighting as Ransomware operators

Targeting

Strategic rivals: U.S.A, Russia, India, Europe

Near neighbors: Taiwan, Japan, South East Asia

Shared Tools

Same tools used by multiple groups, including:

PlugX (aka KorPlug, ShadowPad)

Economic

Targeting of manufacturing, engineering, pharmaceuticals, it services

Tactics

DLL sideloading

Reuse of tools & infrastructure

Noisy. Unconcerned with attribution

Extortion

RA World ransomware

Russia

Shuckworm group

Unit of Russian Federal Security Service (FSB)

Based in Sebastopol, Crimea

Specializes in attacks against Ukraine

Unsophisticated but persistent

High volume of attacks

Indiscriminate

Also known as

Gamaredon, Armageddon, Primitive Bear

Toolset

VBS droppers, custom Pterodo backdoor, USB worms.

Phishing

Emails claiming to contain updates on war, criminal proceedings, protection of children etc.

Tactics

Frequent retooling to avoid detection

Multiple infections for crude persistence

Risks

Lots of collateral victims

Pressure for results

North Korea

Stonefly group

Elite unit linked to military intelligence agency, Reconnaissance General Bureau (RGB)

Specializes in sophisticated espionage attacks against high value targets

Sister groups focus on cryptocurrency theft

Recent years:

Extortion attacks against U.S. organizations

- Healthcare
- SMB companies

Also known as

Onyx Sleet, Andariel, APT45, Silent Chollima

Custom Tools

Custom written Preft backdoor leveraged in extortion and espionage attacks

Extortion

Maui Ransomware

Indictment

July 2024: Indictment linking Stonefly to extortion attacks & naming members

Funding

Espionage attacks against government, military and defense targets including NASA and Air Force bases

Iran

Druidfly group

Specialist in destructive attacks

Targets countries deemed hostile to Iran, including Albania, Israel

Attacks on U.S. a risk

Seedworm group

Classic espionage operation

Linked to the Iranian Ministry of Intelligence and Security (MOIS)

Occasionally deploys DarkBit ransomware

Masquerading

Pretends to be hacktivist groups, e.g. Homeland Justice, Karma

Toolset

Exploits, custom backdoors, remote desktop tools

Social Engineering

Multiple actors with adept social engineering capability, maintaining personas across multiple platforms

Wipers

BibiWiper

ZeroCleare

“Ransomware”

DarkBit ransomware

Cover for destructive attacks

What Can You Do?

Back to Basics with a Twist

We'll dive into two key defensive use cases that highlight how people, process and technology need to execute at a high level across the attack chain

Prevention + Attack Surface Reduction

- Advanced attackers employing LOTL strategies confuse defenses with legit tools
- Augmenting Endpoint Protections with Adaptive Mitigations
- Shifting prevention farther left

Detection + Advanced Response & Forensics

- Understanding the signal from the noise
- Maintaining data to surface correlations and attack patterns that can help mitigate persistent actors
- Track activity across the infrastructure to sanitize any lingering presence

RSAC | 2025 Conference

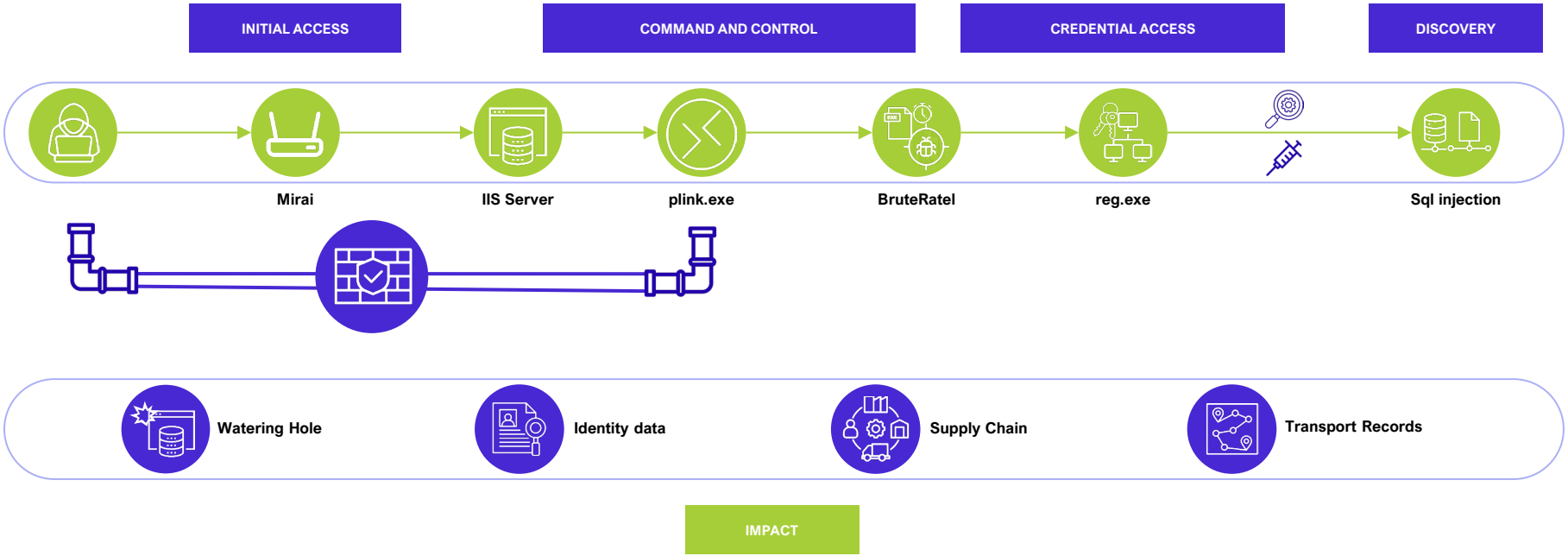
02
Real World Example: Prevent

Many Voices.
One Community.

SeedWorm

- Seedworm (also known as MuddyWater) is a cyber attack group publicly reported to be part of Iran's Ministry of Intelligence and Security
- Highly active since 2017
- Primarily targets organizations in the Middle East
- Targets include government, defense, energy, and telecommunications
- A recent campaign tentatively linked to Seedworm focused on smaller organizations including organizations in utility, transport, and the manufacturing sector outside the Middle East

SeedWorm: Attack Chain



Prevention

Notable attack chain elements

- Living off the land and dual use tools
- Use of exploits north-south and east-west

Living off the land and dual use tools are difficult to block

- One-size-fits-all security solutions are no longer adequate
- Requires a shift in prevention paradigm that adapts to your organization
- Able to recognize legitimate usage of dual-use tools vs malicious usage

Network exploit usage requires Intrusion Prevention not only north-south, but also east-west

Prevention: Adaptive in Action

- Adaptive Protection compares the use of dual-use tools in your environment versus known attacker usage
- Organizations can deny attacker behaviors while still allowing legitimate usage
- Most of our organizations can remove half of the attack surface on day one with zero business impact
- Removing half an attacker's playbook, disrupts almost all threat actors
- This allows security teams to permit legitimate activity of a tool, while also being able to prohibit other behaviors that could malicious
- Your security posture adapts to your organization and is not one-size-fits-all

Prevention: Endpoint Intrusion Prevention

Intrusion Prevention is needed at workstation and server endpoints

Ability to parse inbound network traffic for use of known and zero-day exploits

- Not just outbound endpoint URL reputation

Able to prevent both north-south and east-west exploitation

Provides prevention far left in the attack chain eliminating costly remediation response post access

- Symantec data shows IPS was responsible for 96% of all threat detections

Endpoint intrusion prevention allows prevention of:

- Lateral traverse
- Discovery
- Exploitation of internal and external facing servers

RSAC | 2025 Conference

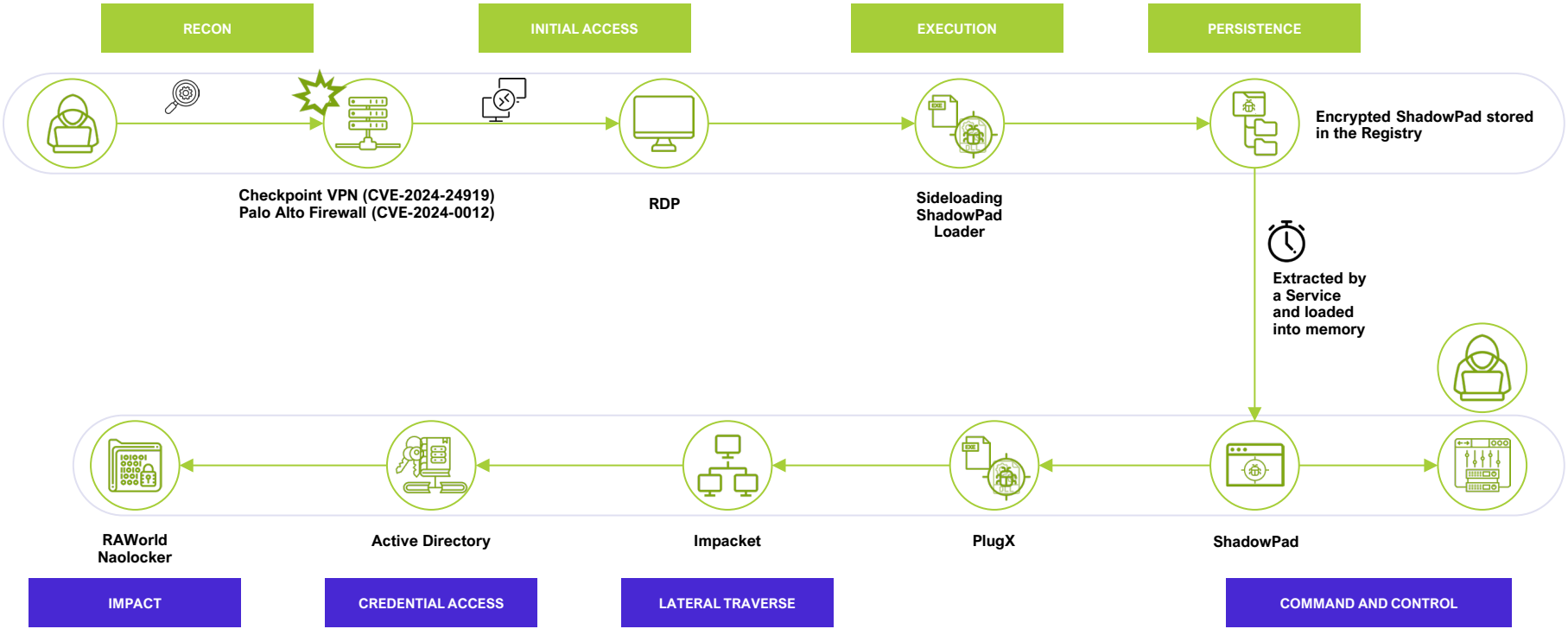
03
Real World Example: Response and Forensics

Many Voices.
One Community.

Moonlighting China-linked APT Group

- Dozens of documented China-linked APT groups
- Primarily focused on national security related espionage, military intelligence, and economic espionage
- Heavy interest in Southeast Asia and Taiwan
- Frequently organizations in healthcare, manufacturing, technology, transport, and telecommunications are victims as part of supply chain or economic espionage attacks
- However, recently we have seen a China-linked group appear to moonlight for direct economic gain deploying ransomware

Moonlighting China APT Group: Attack Chain

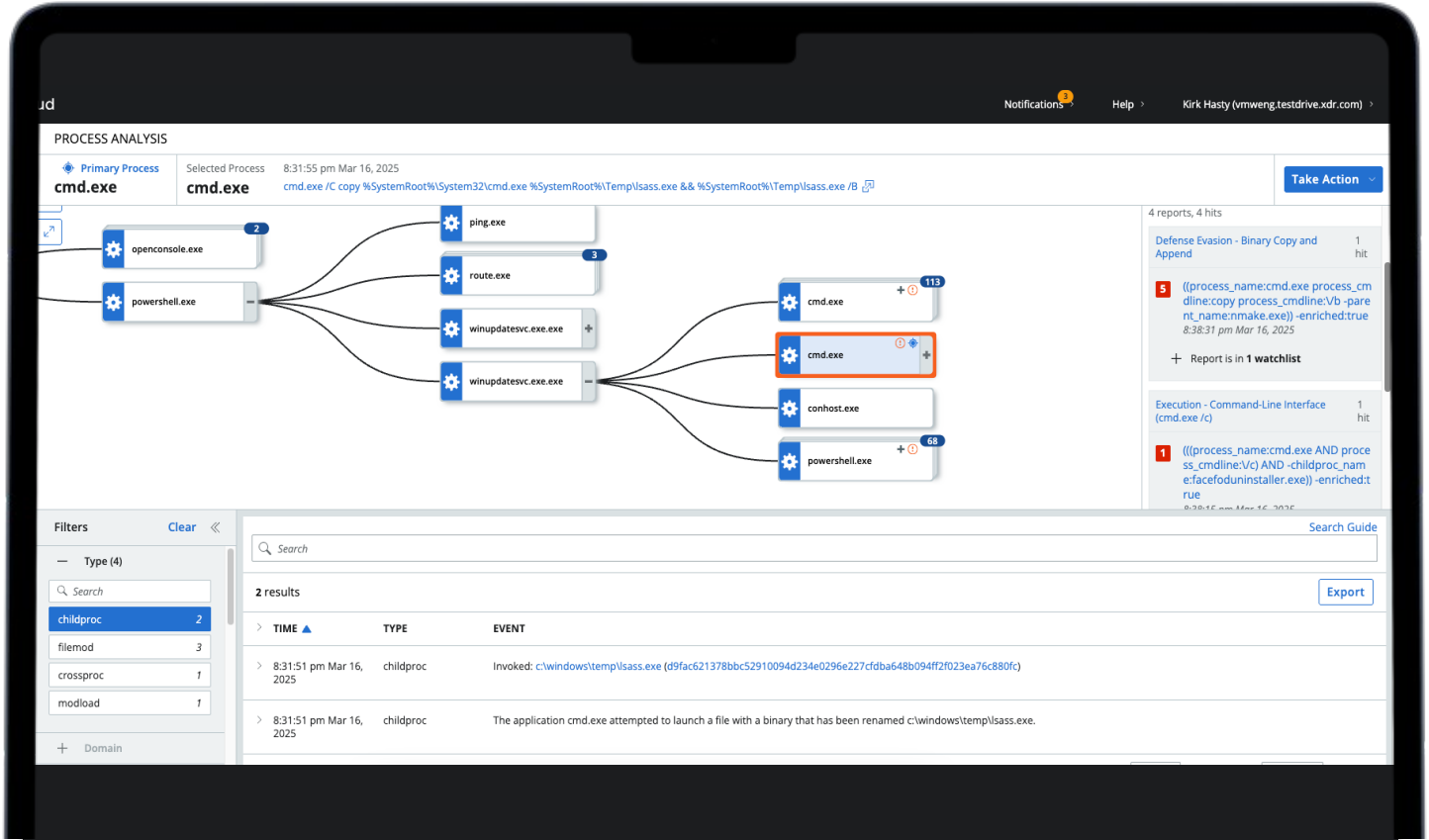


Detection & Response

Notable attack chain elements

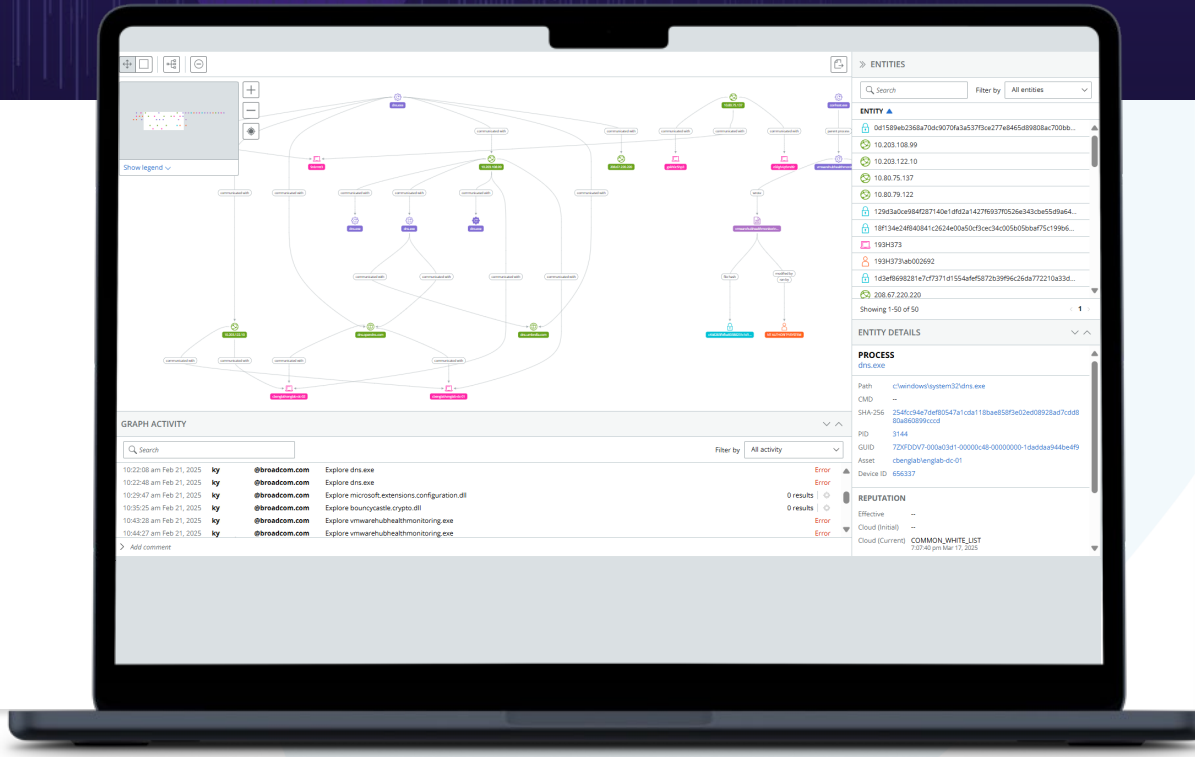
- Multiple distinct techniques used across multiple machines in the organization
- Activity across multiple device types including VPNs, firewalls, servers and endpoints
- Actor accesses or modifies numerous systems including Active Directory credentials, RDP policies, system registries, and system memory
- Network activity includes use of exploits north-south as well as east-west

Detection & Response



Endpoint Detection & Response:

- Continuously record endpoint activity to provide detailed forensic data for investigation
- Build connections to see what happened at every stage of an attack and identify root cause faster
- Isolate infected systems and remove malicious files to prevent lateral movement

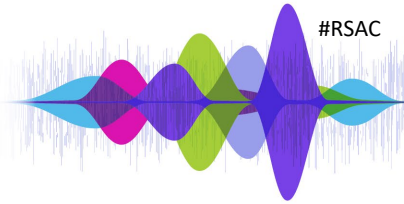


RSAC 2025 Conference

RSAC 2025 Conference

04
Defending Against a Siege

Many Voices.
One Community.



No Easy Button

Fortifications

Ultimately excellence in executing the fundamental controls with help from technology

- Network Security
- Information Security
- Cloud Security
- Application Security
- And of course Endpoint Security

Targeted Defense through Prediction

Mitigations such as disabling the network, disabling user accounts, and quarantining workstations and servers are disruptive to the business

What if you could predict what the attacker was going to do next and simply block their next steps?

Predictive Security:
How it Works

Predictive Security is now possible and was inspired from LLMs

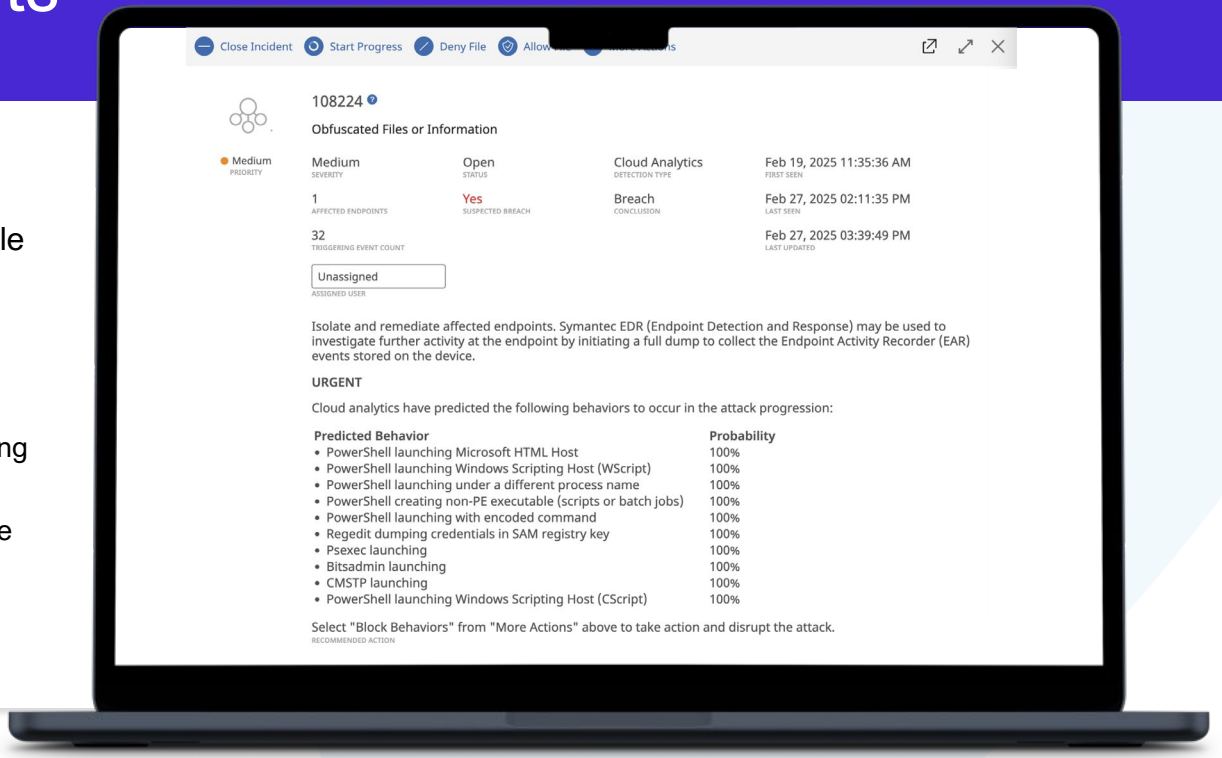
- Large Language Models (LLMs) ingest the text of the Internet
- When composing replies, they predict statistically what is the next word
  - At 8am, the boy went to _____
- Attack chains are analogous to a sentence, each event a word
  - An attachment in email, accessed lsass to steal credentials, contacted a command and control server…

All suspected new attacks are fed into the model, which can now predict statistically the next steps the specific attacker will take

We train on **500,000 attack chains** and build an AI model similar to a LLM

Predictive Security: Results and Benefits

- In our real-world deployment, accurate predictions were available in 80% of incidents
- Predictive Security technology:
  - Disrupts the attacker from completing their goals
  - Buys time for the SOC to investigate
  - Limits disruption to the business


Close Incident
Start Progress
Deny File
108224
Obfuscated Files or Information
Medium
PRIORITY
Medium
SEVERITY
Open
STATUS
Cloud Analytics
DETECTION TYPE
Feb 19, 2025 11:35:36 AM
FIRST SEEN
1
AFFECTED ENDPOINTS
Yes
SUSPECTED BREACH
Breach
CONCLUSION
Feb 27, 2025 02:11:35 PM
LAST SEEN
32
TRIGGERING EVENT COUNT
Feb 27, 2025 03:39:49 PM
LAST UPDATED
Unassigned
ASSIGNED USER
Isolate and remediate affected endpoints. Symantec EDR (Endpoint Detection and Response) may be used to investigate further activity at the endpoint by initiating a full dump to collect the Endpoint Activity Recorder (EAR) events stored on the device.
URGENT
Cloud analytics have predicted the following behaviors to occur in the attack progression:
Predicted Behavior
Probability
PowerShell launching Microsoft HTML Host 100%
PowerShell launching Windows Scripting Host (WScript) 100%
PowerShell launching under a different process name 100%
PowerShell creating non-PE executable (scripts or batch jobs) 100%
PowerShell launching with encoded command 100%
Regedit dumping credentials in SAM registry key 100%
Psexec launching 100%
Bitsadmin launching 100%
CMSTP launching 100%
PowerShell launching Windows Scripting Host (CScript) 100%
Select "Block Behaviors" from "More Actions" above to take action and disrupt the attack.
RECOMMENDED ACTION

RSAC | 2025 Conference

05
What you CAN do

What You CAN Do

Immediate Actions

- Recognize that more advanced threats targeting organizations farther down market is the new reality and adjust your threat model
- Evaluate your environment against this broader threat profile to ensure that you have core coverage across your infrastructure including IPS in east-west
- Expand consumption of threat intelligence to include APT and nation-state attacks to remain current on tools, tactics, and procedures that can affect your organization

3 Months

- Review users and policies to try and limit your attack surfaces and block internal tools that are enabled but rarely, if ever used
  - Adaptive Security technologies can automate this process
- Ongoing analyst training to be able to respond quickly to advanced tactics and determine exposure to persistent threats can buy time and ensure effective response
  - Predictive Security technologies can automate this process
  - Deploy high integrity forensics capabilities to ensure comprehensive visibility

RSAC | 2025 Conference

Many Voices.
One Community.

Thank You

For the latest security intelligence and best practices please visit Security.com